	Application No.	Applicant(s)
Notice of Allowability	10/025,509	KESSLER ET AL.
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. THI **NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initi of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendments made and entered with a Request for Continued Examination filed 11/13/200*

2. ☒ The allowed claim(s) is/are *1-34*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None of the:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from th International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20070130* .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/13/2006 has been entered.

EXAMINER'S AMENDMENT

An Examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's amendment was given in a telephone interview with Mr. Dan De Vos, telephone no. (408) 720-8300, on February 1, 2007.

Pleas amend the application as follows:

Claims 1, 6-7, 11, & 16-34 should be amended to the claim language as shown below. These amended claims will **replace** claims 1, 6-7, 11, & 16-34 as filed on 11/13/2006:

In claim 1, the amendment filed on 11/13/2006 **has been changed to** -- A computer implemented method comprising: calling a single macro instruction operation from a first processor, the single macro instruction operation representing a plurality of primitive security operations, the single macro instruction operation selected from a group of macro operations

including a first key exchange macro operation, a second key exchange macro operation, a finish

macro operation, and a server full handshake macro operation, wherein the first key exchange

macro operation represents a <u>plurality of</u> primitive security operation<u>s</u> including a decrypt

operation, a group of modular arithmetic operations, and seventy-eight hash operations, the

second key exchange operation macro represents a <u>plurality of</u> primitive security operation<u>s</u>

including one decrypt operation, a group of modular arithmetic operations, and twenty-two hash

operations, the finish operation macro represents a <u>plurality of</u> primitive security operation<u>s</u>

including one decrypt operation, an encrypt operation, <u>and</u> twelve hash operations, and the server

full handshake operation macro represents a <u>plurality of</u> primitive security operation<u>s</u> including a

decrypt operation, two encrypt operations, a set of modular arithmetic operations, and thirty-five

hash operations; executing the plurality of primitive security operations at a second processor in

response to receiving the single macro instruction operation from the first processor, the second

processor having a plurality of execution units that each can perform the single macro instruction

operation, wherein a single execution unit of said plurality of execution units performs the

plurality of primitive security operations that correspond to the single macro instruction;

generating a set of data from executing the plurality of primitive security operations at the

second processor; and establishing a secure session <u>between a first network element and a second</u>

<u>network element</u> [[with]] <u>using</u> the set of data<u>, wherein the first network element includes the</u>

<u>first processor and the second processor</u>.--.

In claim 6, the amendment filed on 11/13/2006 **has been changed to** -- A computer

implemented method comprising: calling a single macro security operation from a first processor

to a second processor, the single macro security operation representing a set of primitive security

operations, wherein the single macro security operation is a server full handshake macro

operation; performing the set of primitive security operations in response to the single macro

security operation, the set of primitive security operations comprising, generating a secret and a

key material <u>using at least twenty hash primitive security operations</u>, creating a first finished

hash for a client message <u>using at least four hash primitive security operations</u>, creating a second

finished hash for a server message <u>using at least four hash primitive security operations</u>, creating

a finished message <u>using at least one encrypt primitive security operation and two hash primitive</u>

<u>security operations</u>; and establishing a secure session <u>between a first network element and a</u>

<u>second network element using data generated by performing the set of primitive security</u>

<u>operations in response to the single macro operation, wherein the second network element</u>

<u>includes the first processor and the second processor.</u>

In claim 7, the originally presented claim appearing in the amendment filed on

11/13/2006 **has been changed to** -- The computer implemented method of claim 6 wherein the

set of operations further comprises decrypting a pre-master secret <u>using at least an RSA primitive</u>

<u>security operation</u>; and decrypting a client finished message <u>using at least a decrypt primitive</u>

<u>security operation and a plurality of hash primitive security operations</u>.

In claim 11, the amendment filed on 11/13/2006 **has been changed to** -- A system

comprising: a first network element to request a secure session; and a second network element

networked to the first network element, the second network element to call a macro security

operation from a first processor, the macro security operation associated with a plurality of

primitive security operations, to execute the plurality of primitive security operations at a second

processor in response to the macro security operation, and to generate a set of data from the

execution of the plurality of primitive security operations in response to the macro security operation <u>to establish the secure session between the first network element and the second network element, the macro security operation</u> selected from a group of macro operations including a first key exchange macro operation, a second key exchange macro operation, a finish macro operation, and a server full handshake macro operation, wherein the first key exchange macro operation associated with the plurality of primitive security operations including a decrypt operation, a group of modular arithmetic operations, and seventy-eight hash operations, the second key exchange macro operation associated with the plurality of primitive security operations including one decrypt operation, a group of modular arithmetic operations, and twenty-two hash operations, the finish macro operation associated with the plurality of primitive security operations including one decrypt operation, an encrypt operation, <u>and</u> twelve hash operations, and the server full handshake macro operation associated with the plurality of primitive security operations including a decrypt operation, two encrypt operations, a set of modular arithmetic operations, and thirty-five hash operations.--.

In claim 16, the amendment filed on 11/13/2006 **has been changed to** -- A[[n]] ~~apparatus~~ <u>first network element</u> comprising: a first processor to call a macro security operation associated with a plurality of primitive security operations to establish a secure session, the macro security operation selected from a group of macro security operations including a first key exchange macro security operation, a second key exchange macro security operation, a finish macro security operation, and a server full handshake macro security operation, wherein the first key exchange operation associated with the plurality of primitive security operations including a decrypt operation, a group of modular arithmetic operations, and seventy-eight hash operations,

the second key exchange operation associated with the plurality of primitive security operations
including one decrypt operation, a group of modular arithmetic operations, and twenty-two hash
operations, the finish operation macro represents one decrypt operation, an encrypt operation,
and twelve hash operations, and the server full handshake operation macro associated with the
plurality of primitive security operations including a decrypt operation, two encrypt operations, a
set of modular arithmetic operations, and thirty-five hash operations; a second processor coupled
to the first processor, the second processor to perform the plurality of primitive security
operations in response to the macro security operation from said first processor; and a memory
coupled to the first and the second processor, the memory to store a set of data generated by the
second processor, the data used to establish the secure connection between the first network
element and a second network element.--.

In claim 17, the originally presented claim appearing in the amendment filed on
11/13/2006 **has been changed to** -- The ~~apparatus~~ first network element of claim 16 wherein the
second processor comprises: a request unit to fetch and to distribute the macro security
operation; and a plurality of execution units coupled to the request unit, one of the plurality of
execution units to execute the plurality of primitive security operations.--.

In claim 18, the originally presented claim appearing in the amendment filed on
11/13/2006 **has been changed to** --The ~~apparatus~~ first network element of claim 17 further
comprising: the first processor to call a second macro security operation after calling the first
macro security operation; and a second one of the plurality of execution units to execute a second
plurality of primitive security operations corresponding to the second macro security operation

before the one of the plurality of execution units completes execution of the plurality of primitive

security operations.--.

In claim 19, the originally presented claim appearing in the amendment filed on

11/13/2006 **has been changed to** --The ~~apparatus~~ <u>first network element</u> of claim 17 wherein the

one of the plurality of execution units comprises: a microcode unit to translate the macro security

operation into [[a]] <u>the</u> plurality of primitive security operations; an execution queue unit

coupled to the microcode unit, the execution queue unit to queue the plurality of primitive

security operations; a plurality of primitive security operation units coupled to the execution

queue unit, the plurality of primitive security operation units to perform the plurality of primitive

·security operations; and a bus coupled to the plurality of primitive security operation units, the

bus to transmit data.--.

In claim 20, the originally presented claim appearing in the amendment filed on

11/13/2006 **has been changed to** --The ~~apparatus~~ <u>first network element</u> of claim 16 further

comprising the memory to store a set of source data.--.

In claim 21, the amendment filed on 11/13/2006 **has been changed to** -- A[[n]] <u>first</u>

<u>network element</u> ~~apparatus~~ comprising: a first processor to give the command for a macro

security operation associated with a plurality of primitive security operations, the macro security

operation selected from a group including a key exchange operation macro, a finish operation

macro, and a server full handshake operation macro, wherein the key exchange operation macro

associated with the plurality of primitive security operations including one decrypt operation, a

group of modular arithmetic operations, and twenty-two hash operations, the key exchange

operation macro associated with the plurality of primitive security operations including a decrypt

operation, a group of modular arithmetic operations, and seventy-eight hash operations, the

finish operation macro associated with the plurality of primitive security operations including

one decrypt operation, an encrypt operation, <u>and</u> twelve hash operations, and the server full

handshake operation macro associated with the plurality of primitive security operations

including a decrypt operation, two encrypt operations, a set of modular arithmetic operations,

and thirty-five hash operations; a second processor coupled to the first processor, the second

processor comprising a request unit to retrieve the macro security operation associated with the

plurality of primitive security operations, a plurality of execution units coupled to the request

unit, one of the plurality of execution units to perform the plurality of primitive security

operations retrieved by the request unit, the plurality of primitive security operations

corresponding to the macro security operation; and a memory coupled to the first and second

processor, the memory to store a set of data generated by the second processor<u>, the data used to</u>

<u>establish a secure connection between the first network element and a second network element</u>.--

In claim 22, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The <u>first network element</u> ~~apparatus~~ of claim 21 further

comprising the memory to store a set of source data from the host processor.--.

In claim 23, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The <u>first network element</u> ~~apparatus~~ of claim 21 wherein

each of the plurality of execution units comprises: a microcode unit to translate the macro

security operation into the plurality of primitive security operations; an execution queue unit

coupled to the microcode unit, the execution queue unit to queue the plurality of primitive

security operations; a plurality of primitive security operation units coupled to the execution

queue unit, the plurality of primitive security operation units to perform the plurality of primitive

security operations; and a bus coupled to the plurality of primitive security operation units, the

bus to transmit the set of generated data.--.

In claim 24, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The <u>first network element</u> ~~apparatus~~ of claim 21 further

comprising: the first processor to call a primitive security operation; and a second one of the

plurality of execution units to execute the primitive security operations.--.

In claim 25, the amendment filed on 11/13/2006 **has been changed to** -- A machine-

readable <u>storage</u> medium that provides instructions, which when executed by a set of one or

more processors, cause said set of processors to perform operations comprising: executing a

macro security operation at a first one of the set of processors, the macro security operation

associated with a plurality of primitive security operations, the macro security operation selected

from a group including a key exchange macro, a finish macro, and a server full handshake

macro, wherein the key exchange macro associated with the plurality of primitive security

operations including one decrypt operation, a group of modular arithmetic operations, and

twenty-two hash operations, the key exchange operation macro associated with the plurality of

primitive security operations including a decrypt operation, a group of modular arithmetic

operations, and seventy-eight hash operations, the finish macro associated with the plurality of

primitive security operations including one decrypt operation, an encrypt operation, <u>and</u> twelve

hash operations, and the server full handshake macro associated with the plurality of primitive

security operations including a decrypt operation, two encrypt operations, a set of modular

arithmetic operations; executing the plurality of primitive security operations at a second one of

the set of processors in response to the macro security operation; generating a set of data from

executing the plurality of primitive security operations in response to the macro security

operation; and establishing a secure session ~~with~~ <u>using</u> the set of data <u>between a first network</u>

<u>element and a second network element, wherein the second network element includes the set of</u>

<u>one or more processors</u>.--.

In claim 26, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The machine-readable <u>storage</u> medium of claim 25 wherein

the set of data comprises: a set of decrypted data; a set of encrypted data; and a set of hashed

messages.--.

In claim 27, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The machine-readable <u>storage</u> medium of claim 26 wherein

the set of data further comprises a set of random numbers.--.

In claim 28, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The machine-readable <u>storage</u> medium of claim 25 further

comprising the first processor calling a second operation to establish a second secure session.--.

In claim 29, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The machine-readable <u>storage</u> medium of claim 25 wherein

the secure session is an SSL 3.0 session, a TLS session, or an IPSec session.--

In claim 30, the amendment filed on 11/13/2006 **has been changed to** --A machine-

readable <u>storage</u> medium that provides instructions, which when executed by a set of one or

more processors, cause said set of processors to perform operations comprising: calling a single

macro security operation from a first one of the set of processors, the single macro security

operation associated with a set of primitive security operations, wherein the single macro

instruction is a server full handshake macro instruction; performing the set of primitive security

operations at a second one of the set of processors in response to the single macro security

operation, the set of primitive security operations comprising, generating a secret and a key

material using at least twenty hash primitive security operations, creating a first finished hash for

a client message using at least two hash primitive security operations, creating a second finished

hash for a server message using at least two hash primitive security operations, creating a

finished message using at least one encrypt primitive security operation and two hash primitive

security operations; and establishing a secure session between a first network element and a

second network element using data generated by performing the set of primitive security

operations, wherein said second network element includes the set of one or more processors.--.

In claim 31, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** --The machine-readable storage medium of claim 30 wherein

the set of operations further comprises decrypting a pre-master secret using at least an RSA

primitive security operation and decrypting a client finished message using at least a decrypt

primitive security operation and a plurality of hash primitive security operations.--.

In claim 32, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The machine-readable storage medium of claim 30 wherein

the set of operations further comprises generating a set of random numbers.--.

In claim 33, the originally presented claims appearing in the amendment filed on

11/13/2006 **has been changed to** -- The machine-readable storage medium of claim 30 the set of

operations further comprising creating an expected finished message.--.

In claim 34, the originally presented claims appearing in the amendment filed on
11/13/2006 **has been changed to** -- The machine-readable storage medium of claim 30 further
comprising calling a second macro security operation to establish a second secure session.--.

Allowable Subject Matter

I. Claims 1-34 (as amended and presented under "Examiner's Amendment") are allowed.

The following is an Examiner's statement of reasons for allowance: The above mentioned
claims are allowable over the Cited Prior Arts (CPA) of record, taken singly or in combination,
because they fail to anticipate or render obvious the claimed limitations in combination with the
specific added limitation as recited in independent claims 1, 6, 11, 16, 21, 25, 30 and subsequent
dependent claims.

With regards to independent claims 1, 11, 16, 21, 25, and subsequent dependent claims,
the CPA does not teach or suggest a system/method/computer readable storage medium
including the following limitations as claimed: the single macro operation selected from a group
of macro operations, wherein the first key exchange macro operation represents a primitive
security operation including, among other elements, seventy-eight hash operations; wherein the
second key exchange operation macro represents a primitive security operation including, among
other elements, twenty-two hash operations; wherein the finish operation macro represents a
primitive security operation including, among other elements twelve hash operations, and
wherein the server full handshake operation macro represents a primitive security operation
including, among other elements, thirty-five hash operations. Furthermore, the prior arts taken
singly or in combination fail to anticipate or render obvious the following limitations as claimed:

the second processor/network node generating a set of data from executing the plurality of

primitive security operations and using that data in order to establish a secure session between

the two networked elements.

With regards to independent claims 6, 30, and subsequent dependent claims, the CPA

does not teach or suggest a computer implemented method/computer readable storage medium

including the following limitations as claimed: the single macro security operation, wherein the

server full handshake operation is the single macro security operation which comprises at least

twenty hash primitive security operations in order to generate a secret and key material, creating

a first/second finished hash for a client/server using at least two hash primitive security

operations, and creating a finished message using at least two hash primitive security operations.

Furthermore, the prior arts taken singly or in combination fail to anticipate or render obvious the

following limitations as claimed: the second processor/network node generating a set of data

from executing the plurality of primitive security operations and using that data in order to

establish a secure session between the two networked elements.

If Applicants are aware of prior art better than the CPA of record, they are required to call

the Examiner's attention to these references. Furthermore, any comments considered necessary

by Applicants must be submitted no later than the payment of the issue fee and, to avoid

processing delays, should preferably accompany the issue fee. Such submissions should be

clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nadia Khoshnoodi
Examiner
Art Unit 2137
2/2/2007

NK